REMARKS

Claims 1-5, 7, 9-14, 16 and 18 are pending in the present application. Claims 1 and 10 are amended above. No new matter is added by the claim amendments. Entry is respectfully requested.

Claims 1-5, 7, 9-14, 16 and 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Carson (U.S. Patent Number 6,477,124) in view of Weldon, *et al.* (U.S. Patent Number 6,747,930). Reconsideration of the rejections and allowance of claims 1-5, 7, 9-14, 16 and 18 are respectfully requested.

In the present invention as claimed in independent claim 1, a method of determining the presence of an anomaly region in a digital medium includes performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results, calculating corresponding digital signatures based on data values of the read data segment for each of the multiple read data results, and determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value. If a predetermined number of the digital signatures are not equal in value, the anomaly region is determined to be present.

In the present invention as claimed in independent claim 10, a system for determining whether an anomaly region is present in the digital medium that includes a read unit for performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results, a calculating unit for calculating corresponding digital signatures based on read data values for each of the multiple read data results, and a determining unit for determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value. If a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present.

The Office Action, at page 2-page 3 appears to refer to the "data rate profile" of Carson as being analogous to the "digital signature" of the present invention of claims 1 and 10. Along these lines, the Applicants refer the Examiner to the specification as filed at page 31, line 22 through page 32, line 6, regarding the calculation of a digital signature. In the present invention as claimed in independent claims 1 and 10, the digital signatures are calculated based on the actual, underlying data values of the read data segment. In Carson, the values of the underlying data are not of significance to the process; rather, in Carson, the data rates at which data are written to and read from a disk are used.

As stated in Amendment A dated February 15, 2008, Carson discloses, at column 5, lines 7-25, that data on an optical disk can be read from beginning to end or from "lead-in" to "lead-out," or can be accessed in a non-contiguous fashion. Carson further discloses, at column 8, lines 7-43 and at column 9, lines 14-67, a process for disk authentication based on a data rate at which data are written to and read from a disk. In Carson, a data rate profile indicative of the data rate at which data are written to the disk is stored on a disk and used for disk authentication. The data are intentionally written at different, or varying, speeds, at different locations on the disk, and a measured data rate as a function of position on the disk is used to create the data rate profile. Variance in the data rate at which data are written to the disk results in the pits and lands written to the disk having different sizes, depending on the velocity of the disk at the time and position at which the given pits and lands are written. Authentic disks will include data that are recorded in accordance with the data rate profile and non-authentic disks will not. During playback, a readback system will attempt to speed up and slow down the rotation of the disk to maintain a substantially constant recovered data rate. The behavior of the readback system during readback is monitored, recorded, and analyzed to form a data rate profile for the disk in question. When an unauthorized duplicate disk is created, the expected data rate profile will not be present on the unauthorized duplicate disk because an unauthorized disk will not have variance in the lengths of its pits and lands at expected locations on the disk. During a subsequent reading operation of a disk, the actual velocity of the disk at certain locations can be compared to the expected velocity at those locations to authenticate the disk. If a mismatch occurs, the disk is determined to be an

unauthorized disk and access to the disk can be prevented. If no mismatch is detected, full disk access can be granted.

Carson fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium that includes "calculating corresponding digital signatures based on data values of the read data segment for each of…multiple read data results," and "determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present," as claimed in independent claim 1. Carson further fails to teach or suggest a system for determining the presence of an anomaly region in a digital medium that includes "a calculating unit for calculating corresponding digital signatures based on data values of the read data segment for each of…multiple read data results," and "a determining unit for determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present," as claimed in independent claim 10.

The Office Action dated June 9, 2008 states that a continuous read process in Carson will provide second data at a different, nominal data rate as compared to the rate for an authorized disk, and that the data rate profile of Carson stores different data rates used for disk authentication. In the invention as claimed in claims 1 and 10, the "digital signatures" are calculated "based on <u>data values of the read data segment</u> for each of the multiple read data results." That is, the actual <u>data values of the underlying data of the data segment</u> that is read during the multiple read operations is used to calculate the digital signatures. Carson does not teach or suggest this feature. Instead, in Carson, the authentication process is based on the <u>rate</u> at which data are written to and read from the disk. In Carson, there is no significance to the underlying data values in authenticating the disk. The rate at which data are written to and read from the disk of Carson is not the same as a data value of the data segment which is read during a read operation on the data

segment, as claimed. In addition, the Office Action dated June 9, 2008 acknowledges at page 3, that "Carson does not explicitly disclose in detail about calculating digital signatures based on the different data rates".

Further, as stated in Amendment A dated February 15, 2008, in the invention as claimed in claims 1 and 10, an anomaly region is determined to be present on the disk in the event that a predetermined number of the digital signatures resulting from the underlying data read during the multiple read operations are "not equal in value," or different. In contrast, Carson teaches the inverse; namely that an anomaly region (different sized pits and lands) is determined to be present on the disk in the event that the data rate profiles (measured and expected) are determined to be equal in value, or the same. In addition, as stated above, the Office Action dated June 9, 2008 acknowledges at page 3, that "Carson does not explicitly disclose in detail about calculating digital signatures based on the different data rates". Carson merely measures data rates at which data are written to and read from the disk. There is no calculation of a digital signature based on the underlying data values in Carson, and, therefore, no determination of the presence of an anomaly based on a digital signature.

The Office Action indicates that Weldon, *et al.* discloses "using a digital signal to authenticate if a medium is an original copy or an unauthorized duplicate copy". The Office Action refers to Weldon, *et al.* column 32, lines 46-67, column 7, lines 3-25 and column 30 line 58 through column 31, line 20 for support for this assertion regarding Weldon, *et al.*

With regard to the embodiment of Weldon, *et al.* described at column 32, lines 46-67, a data card includes data stored in a combination of data storage mediums including a swipable magnetic strip portion and an optical storage portion. One side of the data card operates like a credit card and includes, on an outer surface, a magnetic strip for storing data to be read by a swiping machine, a hand-written signature, and imprinted identification information including name, expiration date and card holder identification. The other side of the data card includes an optical data storage area which can be read by an optical reader.

9

With regard to the embodiment of Weldon, *et al.* described at column 7, lines 3-25, Weldon, *et al.* discloses a method and apparatus which prohibit unrestricted duplication of information on an optical medium in which a user manually effects a physical change to the optical disk during an initial use of the optical disk. In this embodiment of Weldon, *et al.* the user may activate or perform a predetermined procedure for rendering one or more predetermined areas or locations of the optical disk unreadable or more error prone. This, in effect, "marks" the optical disk both visually to the user and computationally to a program that accesses information on the optical disk as having been previously accessed. Thus, in a subsequent attempt to access the information on the optical disk, it is possible to determine that the information on the optical disk has been previously accessed due to a change in the information on the disk. For example, during the subsequent access, the optical reader may detect a greater number of read errors than when the optical disk was first accessed.

With regard to the embodiment of Weldon, *et al.* described at column 30, line 58 through column 31, line 20, one or more portions of an optical disk surface are intentionally physically altered during the manufacturing process for the purpose of generating either a correctable or uncorrectable defect during an attempted read of one of the physically altered portions of the optical disk.

Like Carson, Weldon, *et al.* fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium that "calculating corresponding digital signatures based on data values of the read data segment for each of...multiple read data results," and "determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present," as claimed in independent claim 1. Like Carson, Weldon, *et al.* further fails to teach or suggest a system for determining the presence of an anomaly region in a digital medium that includes "a calculating unit for calculating corresponding digital signatures based on data values of the read data segment for each of...multiple read data results," and "a

determining unit for determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present," as claimed in independent claim 10.

There is no teaching or suggestion in Weldon, *et al.* that digital signatures are calculated "based on data values of the read data segment for each of...multiple read data results" as claimed in claims 1 and 10. In addition, in Weldon, *et al.*, there is no teaching or suggestion that digital signatures of multiple read operations are compared to each other or that the comparison is used to determine whether an anomaly is present on the disk, as claimed in claims 1 and 10.

Specifically, in the embodiment described at column 32, lines 46-67 of Weldon, *et al.*, no digital signature is calculated. Rather, in this example, the data card is signed by a human with a hand-written signature, similar to the manner in which a signature is applied to a credit card. This is not a digital signature and there is no teaching in Weldon, *et al.* of calculating a digital signature as a result of the hand-written signature. In addition, in this example of Weldon, *et al.*, the mere disclosure of storing data in an optical strip and on an optical medium does not teach or suggest a digital signature. In Weldon, *et al.* there is no teaching or suggestion of calculating a digital signature and no teaching or suggestion of comparing the digital signatures from the multiple read results.

In the embodiment described at column 7, lines 3-25 of Weldon, *et al.*, no digital signature is calculated. Rather, Weldon, *et al.* discloses that a user manually effects a physical change to the optical disk during an initial use of the optical disk which causes subsequent reading operations to have a change in the number of errors relative to the initial reading operation. In this embodiment of Weldon, *et al.*, the number or errors encountered during a previous read operation are compared to the number of errors incurred in a current read operation. The number of errors incurred in a read operation is not a digital signature which is calculated based on data values of the read data segment, as claimed in claim 1 and 10. There is no teaching or suggestion in Weldon, *et al.* of

11

calculating a digital signature based on data values of the data segment for each of multiple read data results and no teaching or suggestion of comparing the digital signatures from the multiple read results, as claimed in claims 1 and 10.

In the embodiment described at column 30, line 58 through column 31, line 20 of Weldon, *et al.*, no digital signature is created. Rather, in this embodiment of Weldon, *et al.*, one or more portions of an optical disk surface are intentionally physically altered during the manufacturing process for the purpose of creating either a correctable or uncorrectable defect during an attempted read of one of the physically altered portions of the optical disk. The disk is verified to be authentic if the defects reside within some specific area of the optical disk. The determination in Weldon, *et al.* as to whether a defect resides in a specific area is not a digital signature which is calculated based on data values of the read data segment, as claimed in claims 1 and 10. In Weldon, *et al.*, there is no teaching or suggestion of calculating a digital signature based on data values of the data segment for each of multiple read data results and no teaching or suggestion of comparing the digital signatures from the multiple read results, as claimed in claims 1 and 10.

The combination of Carson and Weldon, *et al.* fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium that includes "calculating corresponding digital signatures based on data values of the read data segment for each of...multiple read data results," and "determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, if a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present," as claimed in independent claim 1, and a system for determining the presence of an anomaly region in a digital medium that includes "a calculating unit for calculating corresponding digital signatures based on data values of the read data segment for each of...multiple read data results," and "a determining unit for determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, if a predetermined number of the digital signatures are not equal in

value, the determining unit determining the anomaly region to be present," as claimed in independent claim 10.

Since neither of Carson and Weldon, *et al.* teach or suggest the limitations of independent claims 1 and 10, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 1 and 10 under 35 U.S.C. 103(a) as being unpatentable over Carson and Weldon, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 2-5, 7, 9, 11-14, 16 and 18, it follows that this claim should inherit the allowability of the independent claims from which they depend.
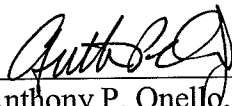
Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

In connection with the foregoing matter, please charge any additional fees which may be due, or credit any overpayment, to Deposit Account Number 50-1798.

Respectfully submitted,

Date: _October 9, 2008_

Mills & Onello, LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900, Ext. 4902
Facsimile: (617) 742-7774
J:\ECD\0014CIP\amendmentb.doc

Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant

13